防火墙实现原理与应用部署研究

摘　要：防火墙技术是网络安全防护中的重要一环，本文对目前网络安全领域主流的防火墙技术实现原理和部署方式进行了分析对比，对应该关注的防火墙指标进行了梳理，并提出了考量标准的建议，对下一代防火墙的发展趋势进行了研究，可在网络安全防护体系建设中用作参考。

关键词：信息安全，防火墙
中图法分类号：TP309.5　　**文献标识码：**A
文章编号：1671-0134（2019）01-107-04　　**DOI：**10.19483/j.cnki.11-4653/n.2019.01.029

文 / 王宝石

前言

防火墙是建设网络应用过程中不可缺少的一环，不管是面向互联网的网络架构还是处于网络纵深内部的网络架构，都需要使用防火墙技术对网络的不同区域之间的通信进行安全控制。防火墙的作用是隔离外部网络的安全威胁，同时隔离通过内部网络向外部网络泄露敏感数据，保护网络资产不受侵害。

防火墙技术在 20 世纪 80 年代就已出现 [1]，随着网络安全技术的不断发展，防火墙技术也在不断演变和完善。在网络建设时对网络安全防护同步进行安全设计和规划，实现对网络进行全面、科学的防护，需要对网络安全防护中最重要的防火墙进行深入的理解。

1. 防火墙工作原理

防火墙最主要的功能是实现与外部网络逻辑隔离，阻止外部网络的攻击者入侵到内部网络，实现“不该来的不要来”；同时保护内部敏感信息资源，防止内部泄密，实现“无授权的不要访问”。

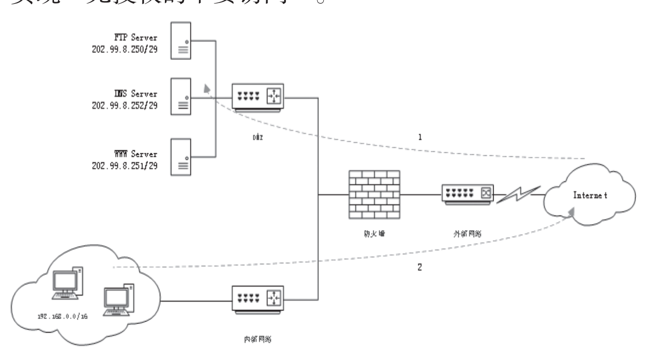


图 1　防火墙对来往数据流量进行过滤

图 1 所示是一个连接互联网的信息系统的典型网络拓扑，系统内部划分为承载着服务的 DMZ 区和用户区，在系统网络出口处部署防火墙与外部互联网连接。防火墙在 1 号数据流量路径上阻止“自己不喜欢”的外部人访问；在 2 号数据流量路径上阻止内部人访问“不应该去”的地方。防火墙不关心访问的具体内容，实现方式是把防火墙部署在网络的出入口处，通过对来往的数据包进行特征判断，对符合安全策略的数据包进行放行，对不符合安全策略的数据包进行丢弃。所以，一般也可以把防火墙称为“安全网关”。

1.1ACL 规则

通过为防火墙配置访问控制列表 ACL（Access Control List）来建立对来往数据包进行判断的规则，防火墙在对数据包进行判断时要通过查询这些规则对数据包进行控制。图 2 所示为防火墙使用访问控制策略对数据包进行控制的工作原理。

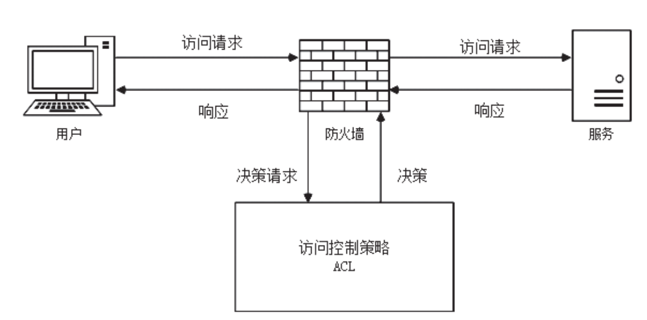


图 2　访问控制策略工作原理

一个标准 IP 访问控制列表的语法为：

access-list [list number] [permit | deny] [source-address] [wildcard-mask] [log]

如下是通过标准 IP 访问控制列表来配置的防火墙策略：

access-list 1 deny 172.16.4.13 0.0.0.0

access-list 2 permit 172.16.0.0 0.0.255.255

access-list 3 permit 0.0.0.0 255.255.255.255

第一条 ACL 表示阻止 172.16.4.13 这台主机的所有流量通过；第二条 ACL 表示允许 172.16 网段的所有数据流量通过；第三条 ACL 表示允许任何地址的数据流量通过。

标准 IP 访问控制列表的定义决定了这种方式的策略只能控制源地址，无法控制数据流量的目的，也无法控制流量的协议。为了实现更加灵活和功能强大的控制方

法，所以出现了扩展 IP 访问控制列表。

扩展 IP 访问控制列表的语法为：

access-list [list number] [permit | deny] [protocol] [source-address] [source-mask] [source-port] [destination-address] [destination-mask] [destination-port] [log] [option]

如下是通过扩展 IP 访问控制列表来配置的防火墙策略：

access-list 150 permit tcp any host 192.168.50.10 eq smtp

access-list 151 permit tcp any host 192.168.50.20 eq www

第一条 ACL 表示允许 TCP 协议的数据包、任何源地址、目的是 192.168.50.10、协议是 SMTP 的数据流量通过；第二条 ACL 表示允许 TCP 协议的数据包、任何源地址、目的是 192.168.50.20、协议是 WWW 的数据流量通过。由此可见，访问控制列表实现的功能就是允许谁到什么地方访问什么服务。

1. 2ACL 规则的匹配原则

在实际应用中，一个完整的信息系统会提供多种服务，进出的数据流量多种多样，因此，在防火墙上会配置多条 ACL。防火墙具备对 ACL 规则的匹配机制来实现对进出流量的匹配，这种机制可概括如下。

防火墙安全规则遵循从上到下匹配的原则，一旦有一条匹配，则对数据包按照该条规则进行处理，剩余的 ACL 不再进行匹配。因此，ACL 的顺序非常重要。

如果所有的规则都没有匹配到，数据包将被丢弃。

安全过滤规则主要包含源、目的地址和端口、TCP 标志位、应用时间以及一些高级过滤选项。

1. 3 防火墙工作方式

1.3.1 包过滤方式

包过滤（Packet Filtering）方式 [2] 是防火墙最早支持的一种方式。防火墙部署在数据流量必须经过的链路上，对经过的每一个数据包逐条匹配 ACL，直到适合某条规则执行规则设定的动作。

不设置内容缓冲区，不关心传输的内容。优点是简单易行，处理速度快；缺点是单包处理，只检查包头，不建立前后数据包的逻辑关系，不能发现通信中插入或缺漏的数据包，也不能发现假冒的数据包。如 TCP 通信三次握手，包过滤方式防火墙不去检查发送的数据包顺序是否合法，因此容易受到 DoS 攻击。

1.3.2 状态检测方式

为了弥补包过滤防火墙天生存在的弱点，后来出现了状态检测方式的防火墙，依据 TCP 标准的协议规则对数据包进行协议检测。状态检测防火墙基于数据包检测，同时针对每个数据连接建立协议运行的状态跟踪，发现状态不匹配时则丢弃该数据包。图 3 所示为状态检测防火墙工作原理。当数据包进入防火墙后，防火墙首先检测该数据包是否匹配已经配置好的状态检测列表，如果匹配则转发放行；如果不匹配则按照包过滤方式安全检测，匹配则转发放行，不匹配则丢弃该数据包。状态检测方式是对包过滤方式的功能扩展，既能对数据包是否符合安全策略进行检查，也能对包的状态进行检测，能够实现对基于破坏数据包状态进行攻击（如 DoS）的防护。

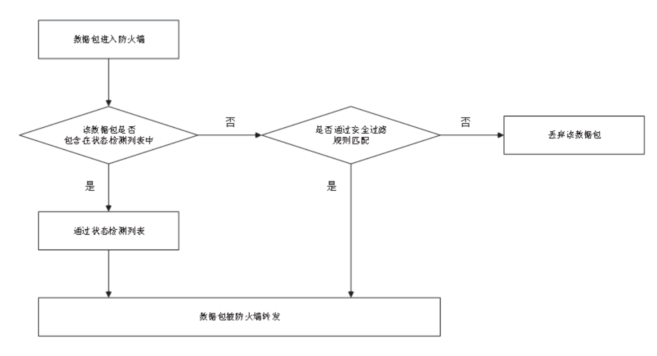


图 3 状态检测防火墙工作原理

状态检测防火墙实现对每一个数据包进行状态检测，需要针对进入防火墙的数据包开启缓冲区。当通过防火墙的数据包数量增多时，会大量占用防火墙硬件资源，降低数据通过性能，有影响业务正常运行的可能。

1.3.3 应用代理方式

在防火墙上开启若干应用代理，每个代理需要一个不同的应用进程或一个后台运行的服务程序，针对每个新的应用必须添加针对此应用的服务程序，否则不能使用该服务，即不代理的业务无法通过。应用代理防火墙的特点是把用户的请求数据包统一收集起来，还原成应用级的请求，对应用级请求按规则进行处理后再转发给服务器，用户向服务器的请求是中断的。应用代理防火墙的优点是成为用户访问业务的中间代理人，中断用户与服务器的直接连接，可以避免对服务器的直接入侵；缺点是需要与包过滤、状态过滤技术一起使用，而且缓冲时间长、速度慢、延迟大。

2. 防火墙部署方式

防火墙是为加强网络安全防护能力在网络中部署的硬件设备，有多种部署方式，常见的有桥模式、网管模式和 NAT 模式等。

2. 1 桥模式

桥模式也可叫作透明模式。最简单的网络由客户端和服务器组成，客户端和服务器处于同一网段。为了安全方面的考虑，在客户端和服务器之间增加了防火墙设备，对经过的流量进行安全控制。正常的客户端请求通过防火墙送达服务器，服务器将响应返回给客户端，用户不会感觉到中间设备的存在。工作在桥模式下的防火墙没有 IP 地址，当对网络进行扩容时无需对网络地址进行重新规划，但牺牲了路由、VPN 等功能。

2.2 网关模式

网关模式适用于内外网不在同一网段的情况，防火墙设置网关地址实现路由器的功能，为不同网段进行路由转发。网关模式相比桥模式具备更高的安全性，在进行访问控制的同时实现了安全隔离，具备了一定的私密性。

2.3 NAT 模式

NAT（Network Address Translation）地址翻译技术由防火墙对内部网络的 IP 地址进行地址翻译，使用防火墙的 IP 地址替换内部网络的源地址向外部网络发送数据；当外部网络的响应数据流量返回到防火墙后，防火墙再将目的地址替换为内部网络的源地址。NAT 模式能够实现外部网络不能直接看到内部网络的 IP 地址，进一步增强了对内部网络的安全防护。同时，在 NAT 模式的网络中，内部网络可以使用私网地址，可以解决 IP 地址数量受限的问题。

如果在 NAT 模式的基础上需要实现外部网络访问内部网络服务的需求时，还可以使用地址 / 端口映射（MAP）技术，在防火墙上进行地址 / 端口映射配置，当外部网络用户需要访问内部服务时，防火墙将请求映射到内部服务器上；当内部服务器返回相应数据时，防火墙再将数据转发给外部网络。使用地址 / 端口映射技术实现了外部用户能够访问内部服务，但是外部用户无法看到内部服务器的真实地址，只能看到防火墙的地址，增强了内部服务器的安全性。

2.4 高可靠性设计

防火墙都部署在网络的出入口，是网络通信的大门，这就要求防火墙的部署必须具备高可靠性。一般 IT 设备的使用寿命被设计为 3 至 5 年，当单点设备发生故障时，要通过冗余技术实现可靠性，可以通过如虚拟路由冗余协议（VRRP）等技术实现主备冗余。目前，主流的网络设备都支持高可靠性设计，如图 4 所示就是一个典型的骨干网络出口处的高可靠性网络架构设计。

3. 防护体系设计

对于网络安全防护来讲，防火墙不是万能的。防火墙只对数据通信的五元组进行检测，不会检查数据包的内容。而攻击者往往会利用各种隐藏掩饰技术将恶意代码放置到合法的数据包中，发送到服务器以达到对服务器进行攻击的目的，如通过把恶意代码放到邮件的附件中发送给目标，这是传统防火墙解决不了的问题。

随着网络应用的愈发广泛，用户希望得到的防护不仅仅限于对访问控制策略的实现，还需要对病毒、蠕虫、木马等恶意代码进行防护。而基于传统的五元组技术的防火墙对于以业务复用方式进行的网络攻击无能为力。

现代安全防护体系提出了下一代防火墙的概念。下一代防火墙具备标准的防火墙功能，如网络地址转换、状态检测、VPN 等功能；具备入侵检测功能；具备应用

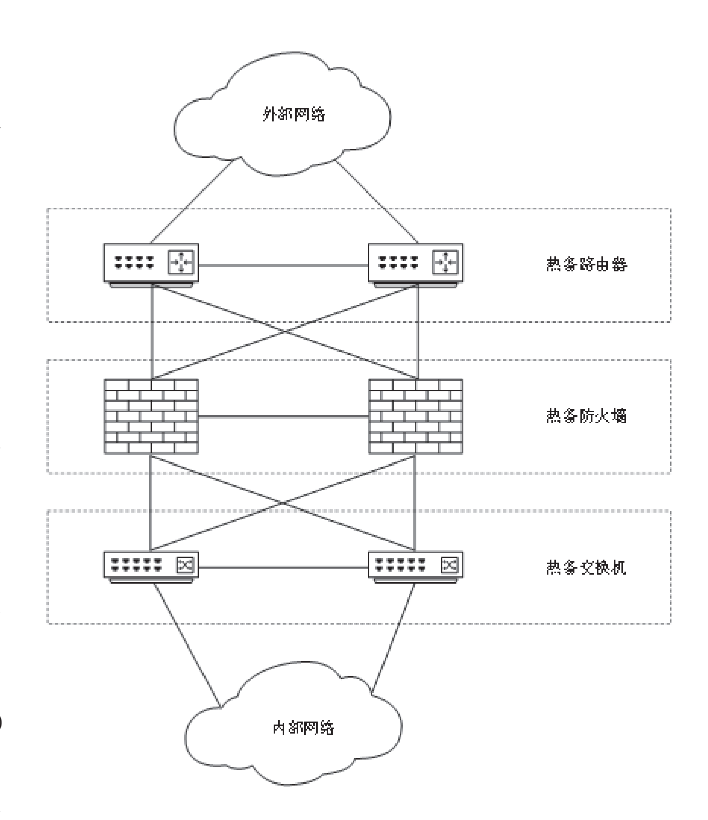


图 4　骨干网络高可用性架构设计

程序感知能力，自动识别和控制应用程序，甚至完成基于用户的数据流量控制功能。所以，现代的安全防护应该由传统的对于五元组的控制转变为以用户身份定义安全策略、识别内容与业务应用的方式，能够基于 MAC 地址、数据流方向、用户身份、内容关键字等因素对流量进行控制，这要求防火墙不仅在网络层进行检测，还应在应用层进行检测。最完整的下一代防火墙技术应包含传统防火墙功能、IPS 功能、恶意代码检测功能，甚至扩展到 VPN、URL 过滤、应用流量控制、WAF、链路负载均衡等功能。

4. 防火墙性能考量

4.1 防火墙性能指标

防火墙无论采用什么方式对数据进行过滤，都是以防火墙的硬件资源作为支撑，防火墙的性能直接影响用户的体验甚至系统安全。防火墙最重要的性能指标包括吞吐量、时延、丢包率、并发连接数、新建连接数等。

吞吐量指防火墙的数据通过能力，根据以太网中数据包的封装规则，以千兆防火墙举例吞吐量应为：

$$64/(64+8+12)*1000\text{Mbps}*1.024 \approx 780.2\text{Mbps}$$

不论防火墙工作在哪种工作方式下，防火墙都要对通过的数据进行处理，比数据在光纤中通过的速度要慢。互联网有大量的网络设备，数据从源到目的经过的时延是通过的所有设备的时延的和。一般防火墙的时延应控制在毫秒级别。

防火墙在处理通过的数据包时，可能会因为错误或

者延迟等原因丢失了部分数据包。这里丢失的数据包不包括因不符合 ACL 策略而被丢弃的数据包，除此之外，有丢失数据包的情况应判定防火墙存在问题。

当通过防火墙的数据出现大量的并发连接和新建连接时，防火墙需要跟踪这些连接的状态，防火墙的 CPU 等硬件资源是否足以支撑这些连接带来的资源消耗，用连接数的形式进行判断。

4.2 虚拟化和策略硬件化

从防火墙的工作原理来看，对防火墙的硬件要求比较高。随着网络的升级，目前千兆、万兆甚至 100G 交换机都应用于网络。在这些高吞吐的网络中对防火墙的性能提出了更高的要求，需要提升防火墙本身采用硬件的性能。同时，防火墙也有一些架构上的设计来应对高吞吐量网络应用。

虚拟化[3]指防火墙设计成具备多组端口，通过软件配置实现一台硬件防火墙可以虚拟成多个虚拟防火墙使用，具备多个防火墙的处理能力。虚拟化还是使用 CPU 执行算法对数据流量进行过滤，处理速度依然受限于 CPU 的处理能力。

策略硬件化指不再使用 CPU 通过算法去处理每一次 ACL 匹配，而是把每一条策略封装成如 FPGA 芯片的方式对数据包进行处理。当有大量的数据包通过时，使用多个 FPGA 芯片组成的硬件规则表对数据包进行过滤，能够大幅度提升数据处理的速度。

结语

在构建网络安全防护体系的过程中，用户需要针对网络架构和业务需求选择适合的防火墙工作模式和部署方式，应该选用具备自身安全需求的防火墙功能，并对防火墙的硬件性能进行考量，使防火墙为网络提供高效、准确的防护服务。

防火墙技术在网络安全领域既是出现最早的技术，也是应用最广泛的技术。随着对网络安全的需求不断增大，防火墙技术在不断进步，防火墙处理能力的高速化、检测能力智能化、部署方式多样化都是防火墙应对网络安全需求的改进方式。在未来，防火墙仍然是网络安全应用最重要的设备之一。媒

参考文献

[1] 张艳．防火墙产品原理与应用 [M]. 北京： 电子工业出版社，2016，1（1）.

[2] 陈波．防火墙技术与应用 [M]. 北京： 机械工业出版社，2016，1（1）.

[3] 谢正兰，张杰．新一代防火墙技术及应用 [M]. 西安：西安电子科技大学出版社， 2018，5（1）.

（作者单位：国家广播电视总局监管中心）

（上接第38页）

久弥新地被反复送上热门——正是在这样一种意义运作中，与外在生产、消费的现实情境形成默契的错位互动而构建神话。

同样，另外一类以百家讲坛式的“业界专家”姿态兜售各种各类“成功经验”（投资理财、创业经商、应聘礼仪、情感生活、职场技能）的热门短视频，不过是在不断翻新地对“胜利者话语”（以马云、俞敏洪、马东、李诞等这些知名既得利益群体为代表）加以打包，面向那些无法认清现况、不切实际渴望暴富或成名的庸俗屌丝进行二手贩卖。然而，这种兜售实际所能满足的不过是这些布衣阶层一时的意淫和过瘾，因为成功是无法复制的。这些充斥于耳的“胜利者话语”必然遮蔽和掩藏了既得利益群体在攫取成功过程背后那些“不可为人知”的捷径和巧合，他们不过是幸运儿或者是幸运儿中的幸运儿。因此，对于并不先在占有物质或文化资源优势的普通人而言，成功是没有捷径的；所谓“成功经验”非但不是捷径桥梁，反而会诱拐那些真正有志向且有能力、原本有可能书写自己专属成功故事的人，最终沦落为一个庸碌的仿效失败者。媒

注释

①尼古拉斯·加恩海姆，贺玉高，陶东风．政治经济学与文化研究 [J]. 西北师大学报（社会科学版），2005（42）.

②尹鸿．大众文化时代的批判意识 [J]. 文艺理论研究，1996（3）.

③陶东风，和磊．文化研究 [M]. 广西：广西师范大学出版社，2006.

参考文献

[1] 罗钢，刘象愚．文化研究读本 [M] 北京：中国社会科学出版社，2000.

[2] 阿雷恩·鲍尔德温．文化研究导论（修订本）[M] 北京：高等教育出版社，2004.

[3] 约翰·斯道雷．文化理论与大众文化导论 [M]. 北京：北京大学出版社，2010.

[4] 艾瑞咨询 .2018 年中国短视频营销市场研究报告 [EB 或 OL]. http： 或 或 report.iresearch.cn 或 report_pdf.aspx?id=3302，2018-12-3 或 2018-12-19.

（作者单位：河南大学民生学院）